42390P7648                                                PATENT

# REMARKS

Applicants respectfully present Claims 1 and 3-20 for examination in the RCE filed herewith. Claim 2 has been canceled herein without prejudice to the filing of continuations and/or divisionals, and Claims 1, 6 and 18 have been amended herein to more clearly define the scope of the presently claimed invention. No new claims have been submitted and no new matter has been introduced. Applicants respectfully submit that the claims and remarks presented herein overcome the Examiner's rejections in the Final Office Action dated January 19, 2005 in the parent application.

### *35 U.S.C. §103*

Claims 1, 3-7, 9-14 and 16-17 stand rejected under 35 U.S.C. §103 as being unpatentable over Calendor (2002/0188567) in view of Kocher et al. (U.S. Patent No. 6,289,455). Additionally, Claims 2 and 8 stand rejected under 35 U.S.C. §103 as being unpatentable over Calendor in view of Kocher and further in view of Kotani et al (2001/0008016). Finally, Claims 18-20 stand rejected under 35 U.S.C. §103 as being unpatentable over Davis (U.S. Patent No. 6,064,739 in view of Wilson (U.S. Patent No. 5,742,680). Applicant respectfully traverses the Examiner's rejections.

The Examiner submits that Calendor discloses a system and method for controlling the reproduction and recording of digital content comprising intercepting a signal from a view transmission, the signal comprising a scrambled content and a decryption key and extracting the decryption key from the signal. The Examiner concedes, however, that Calendore does not teach encrypting the extracted decryption key and storing the encrypted decryption key. The Examiner suggests, however, that Kocher teaches these elements and that that it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the use of encrypting the decruption key and storing the encrypted descryption key as Kocher teaches in the system of Calendor so as to prevent attacks to decryption keys. Applicant strongly disagrees.

First, Applicant respectfully submits that the Examiner improperly combined Calendor with Kocher. Calendor describes a method for simulcrypting scambled data to a plurality of conditional access decides while Kocher describes a method and apparatus for preventing piracy

5

42390P7648                                                                                PATENT

of digital content. The Examiner makes no showing of why it would have been obvious to one of ordinary skill in the art to combine Calendor with Kocher. As set out in M.P.E.P. § 706.02(j), "(t)here must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." Applicant respectfully submits that there is no such motivation. For example, Calendor makes no mention or suggestion of encrypting keys, such that one of ordinary skill in the art would have been motivated to combine the teachings of Calondor with Kocher. The mere fact that both references address aspects of encryption and that, if combined, the references *may* provide a benefit does not prima facie render the combination obvious. Applicant therefore respectfully submits that the combination of these references is improper and respectfully request the Examiner to withdraw the 35 U.S.C. § 103 rejections to Claims 1, 3-7, 9-14 and 16-17.

Even assuming arguendo these references were properly combined, Applicant respectfully submits that they do not render Claims 1, 3-7, 9-14 and 16-17 unpatentable. As the Examiner concedes, Calendore does not teach encrypting the extracted decryption key and storing the encrypted decryption key, but suggests that Kocher teaches these elements. Applicant respectfully submits that as amended, independent Claims 1, 6 and 18 include the elements of extracting the scrambled content from the signal and storing the scrambled content separate from the stored encrypted decryption key. Neither of these elements is taught by Calendore and Kocher, alone and/or in combination. Applicant therefore submits that this rejection is moot.

With respect to Claims 2 and 8, the Examiner submits that these claims are unpatentable over Calendor in view of Kocher and further in view of Kotani. Again, Applicant strongly disagrees. Applicant first points out that the feature of Claim 2 has been incorporated into Claims 1 and 6 thus rendering the rejection to Claim 2 moot. With respect to this feature in Claims 1 and 6, however, Applicant submits that first and foremost, the combination of Calendor and Kocher is improper. Applicant further submits that the combination of Kotani with Calendor and Kocher is also improper for similar reasons. Specifically, Kotani describes an information management method and information management apparatus and nothing in Kotani suggests any motivation to combine Kotani with either Calendor or Kocher. Applicant thus respectfully submits that the combination of these references is improper.

6

42390P7648                                                    PATENT

Even assuming arguendo these references were properly combined, Applicant respectfully submits that the combination of these references does not render Claims 1 and 6 unpatentable. Specifically, the section of Kotani referred to by the Examiner (when read in context of the previous paragraphs) merely describes the process of using information specific to a predetermined area to encrypt various types of information. As described in Kotani:

> "Further, the information management method can be constituted so that when the predetermined information is to be derived outside the first area, it is encrypted by medium-specific information or a key generated therefrom, and by information specific to the apparatus that drives the recording medium or a key generated therefrom.
>
> In such a case, the information management method can be constituted so that the encrypted predetermined information stored in the second area is decrypted by information specific to the apparatus that drives the recording medium or a key generated therefrom, and medium-specific information or a key generated therefrom, and the predetermined information stored in the first area is updated.
>
> By means of such constitution as described above, when predetermined information is derived outside the predetermined area in which it is stored, it is encrypted using information specific to this medium; therefore, it is difficult to decrypt this information, even if it has been copied to a different medium. For example, if, when software or publications and the like are stored in a second area, this electronic data is stored after having been encrypted using an encryption key, and the decryption key for decrypting this is encrypted by information specific to this medium and stored in a first area to which a user has no access, there is no need to change the encryption key for encryption for each individual user, and a common encryption key can be used for encryption and stored. Because the encrypted decryption key stored in the first area is further encrypted using medium-specific information and then derived outside the first area, a user can make and save a backup copy. Because this saved backup data has been encrypted using medium-specific information, it is difficult to decrypt even if copied onto another medium, and thus it is difficult to obtain the decryption key for decrypting the electronic data."

Kotani, Paragraphs 20-22.

It will be readily apparent to those of ordinary skill in the art that these sections of Kotani are directed to ensuring that decryption keys are encrypted with information specific to the medium on which the decryption keys are stored and which a user is unable to access. Kotani makes no mention of storing the scrambled content separate from the stored encrypted decryption key and the section highlighted by the Examiner cannot be read to mean such. Applicant therefore respectfully submits that the combination of Kotani with Calendor and/or Kocher does not render Claims 1 and 6 unpatentable. As a result, dependent Claim 8 is also patentable over the combination of these references and Applicant respectfully respectfully requests the Examiner to withdraw the 35 U.S.C. § 103 rejections to these claims.

Finally, the Examiner rejected Claims 18-20 under 35 U.S.C. §103 as being unpatentable over Davis in view of Wilson. Applicants once again traverse the Examiner's rejection. Davis describes a system and method for copy-protecting distributed video content while Wilson

7

42390P7648                                              PATENT

describes a set top box for receiving, decrypting and descrambling a plurality of satellite television signals. There is no teaching in either Davis or Wilson for extracting scrambled content and decryption keys from a video signal, encrypting the decryption keys and storing the scrambled content and the encrypted decryption keys separately. The sections of the references highlighted by the Examiner, alone or in combination, do not support these claimed elements. Applicant therefore respectfully submits that these references, alone or in combination, do not anticipate Claims 18-20. Applicant therefore respectfully requests the Examiner to withdraw the rejections to Claims 18-20.

In summary, Applicant respectfully submits that all pending claims are patentable over the cited references. As such, Applicant respectfully requests the Examiner to withdraw the rejection to these claims under 35 U.S.C. §103.

8

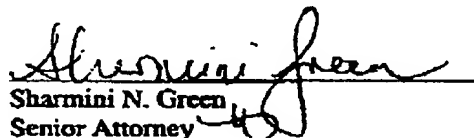42390P7648                                                      PATENT

# CONCLUSION

Based on the foregoing, Applicant respectfully submits that the applicable objections and rejections have been overcome and that pending Claims 1 and 3-20 are in condition for allowance. Applicant therefore respectfully requests an early issuance of a Notice of Allowance in this case. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (310) 406-2362.

If there are any additional charges, please charge Deposit Account No. 50-0221.

Respectfully submitted,

Dated: April 18, 2005

Sharmini N. Green
Senior Attorney
Intel Corporation
Registration No. 41,410
(310) 406-2362

9